CHAPTER – 14

SECURITY AT THE TRANSPORT LAYER: SSL

LEARNING OBJECTIVES

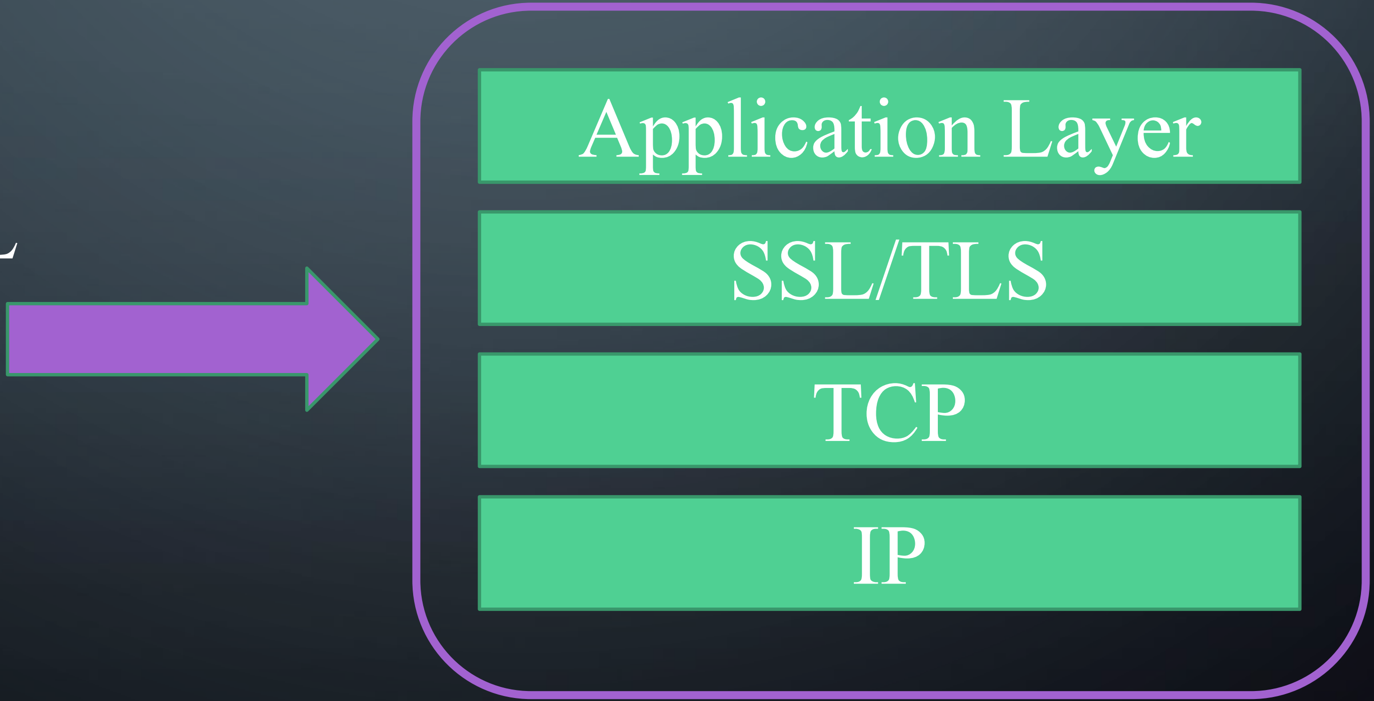
- ✔Discuss the need for security services at the transport layer of Internet Protocol

- ✔Illustrate the general structure of Security Socket Layer (SSL)

SECURITY SERVICE AT TRANSPORT LAYER

- Transport layer security provides end to end security services for applications that use a reliable transport layer protocol such as TCP

Location of SSL
in the Internet
Model



Application Layer

SSL/TLS

TCP

IP

Continue…

Example of online shopping:

- ✓Customer needs to be sure that the server belongs to the actual vendor, not an impostor

Authentication

- ✓Customer and vendor need to be sure that the contents of the message are not modified during transmission

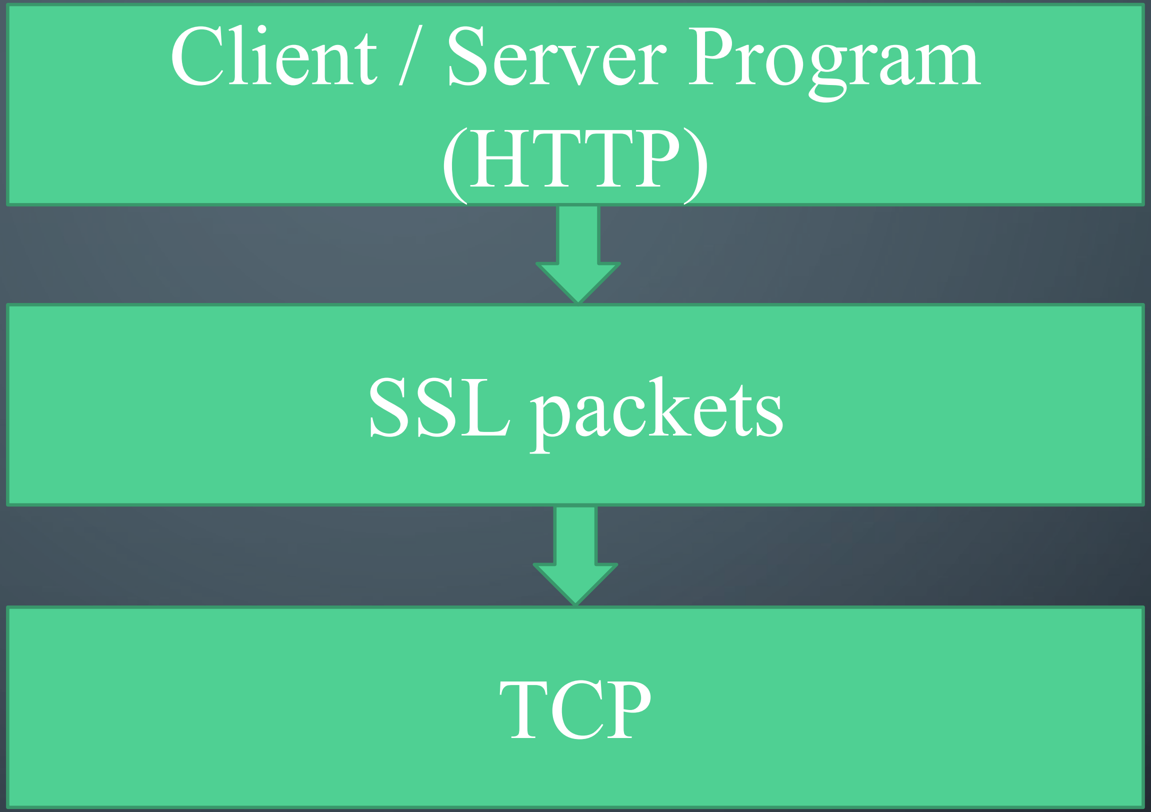
Integrity

- ✓Customer and vendor need to be sure that an impostor does not intercept sensitive information

Confidentiality

Continue…

Working of SSL:



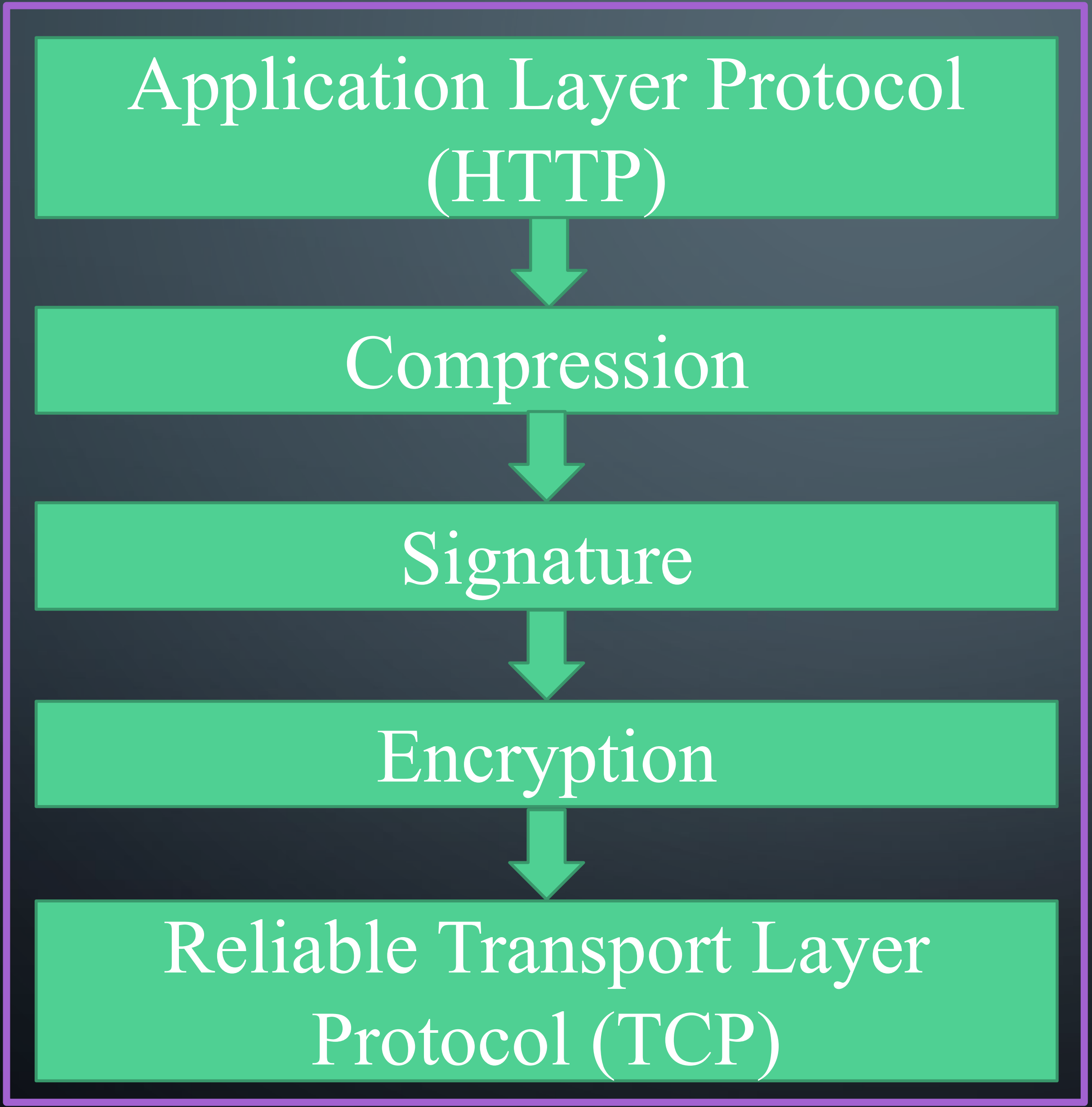
Client / Server Program (HTTP)

SSL packets

TCP

Note: If server & client are capable to run SSL program then the client can use URL – https otherwise http

SSL ARCHITECTURE



Application Layer Protocol (HTTP)

Compression

Signature

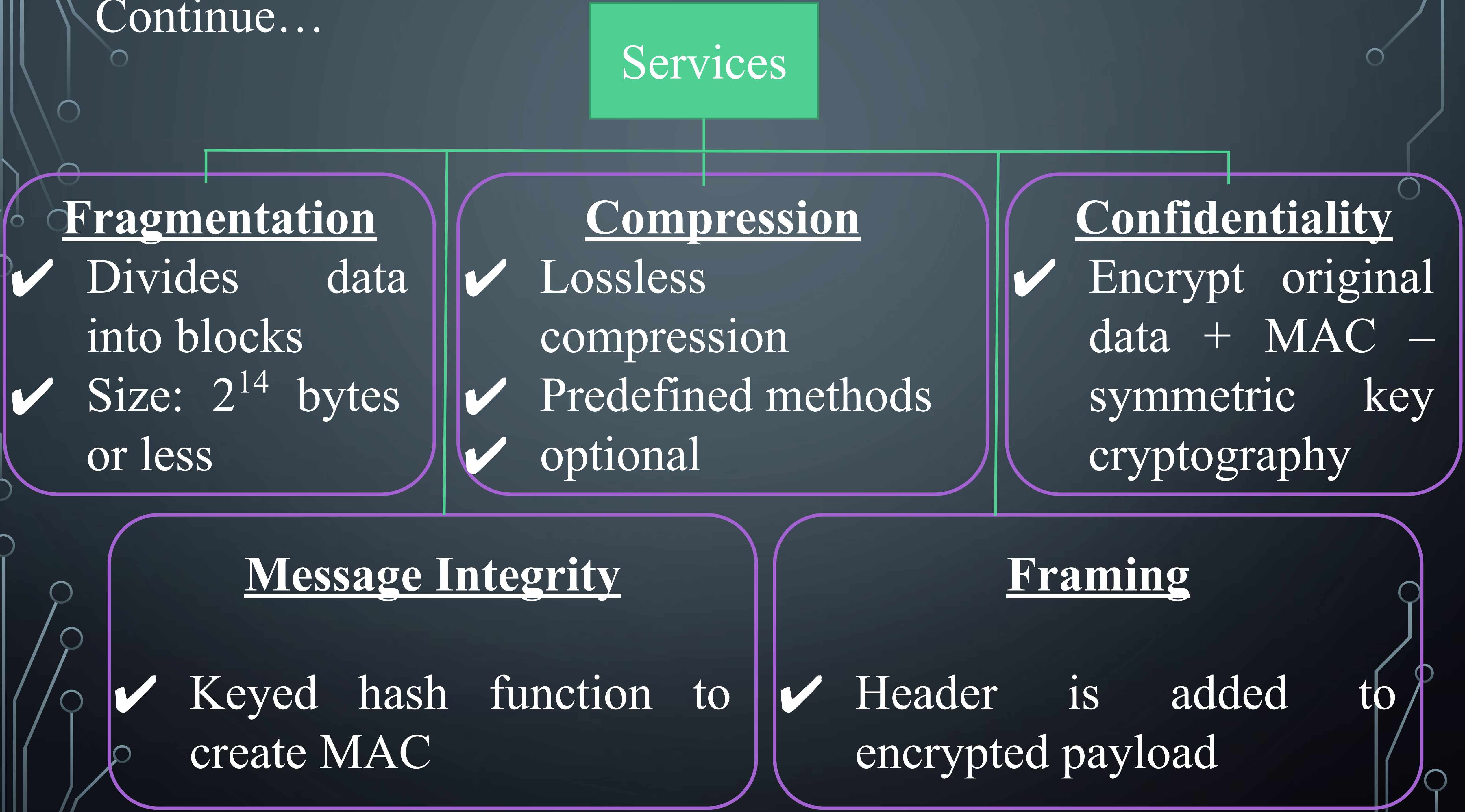
Encryption

Reliable Transport Layer Protocol (TCP)

- ✔ SSL is developed by Netscape in 1994
- ✔ Version 2 & 3 were released in 1995

Note: we will discuss SSLv3

Continue…



Services

Fragmentation

- ✔ Divides data into blocks
- ✔ Size: 2^{14} bytes or less

Compression

- ✔ Lossless compression
- ✔ Predefined methods
- ✔ optional

Confidentiality

- ✔ Encrypt original data + MAC – symmetric key cryptography

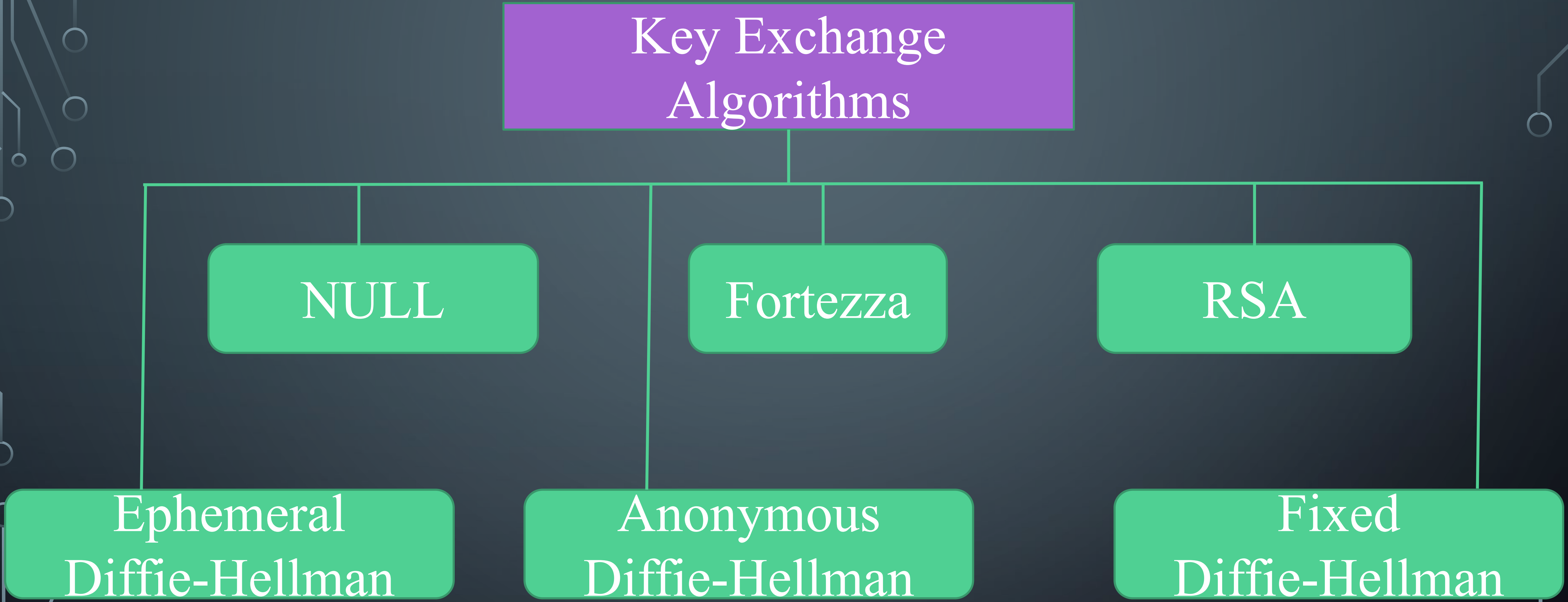
Message Integrity

- ✔ Keyed hash function to create MAC

Framing

- ✔ Header is added to encrypted payload

Continue…



Key Exchange Algorithms

NULL

Fortezza

RSA

Ephemeral Diffie-Hellman

Anonymous Diffie-Hellman

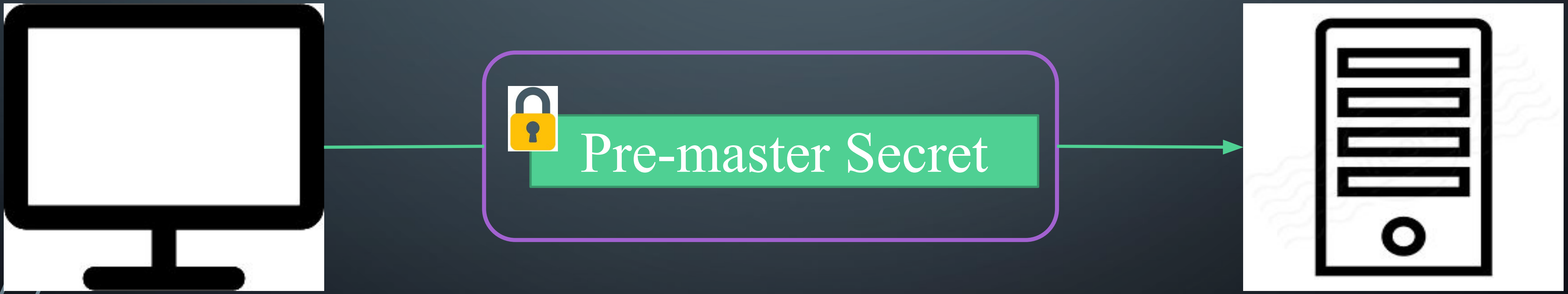
Fixed Diffie-Hellman

Continue…

NULL : no key exchange

no pre-master secret

RSA : pre-master secret – 48 byte random number



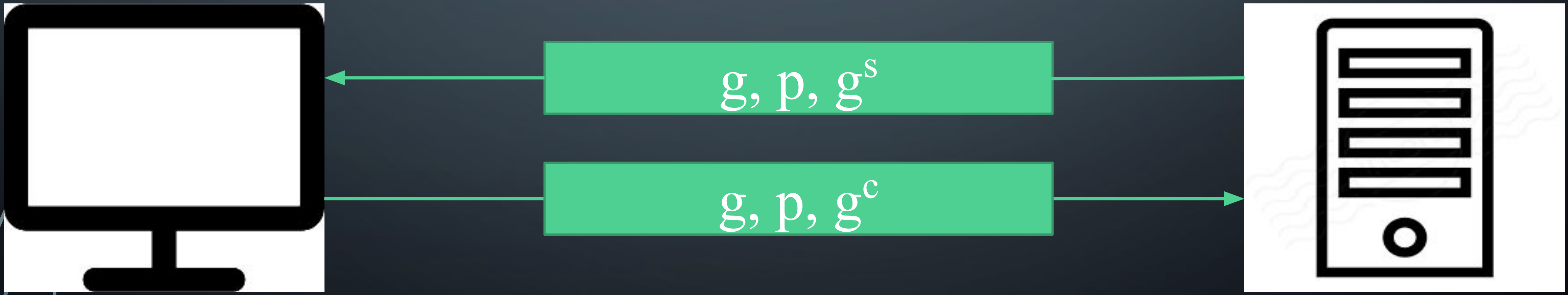
🔒 Pre-master Secret

🔒 - Encrypted with server's public key

Continue…

Anonymous Diffie-Hellman :

- simplest and most insecure method
- pre-master secret using DH
- half keys are sent in P.T.
- neither party is known to the other – man in middle attack

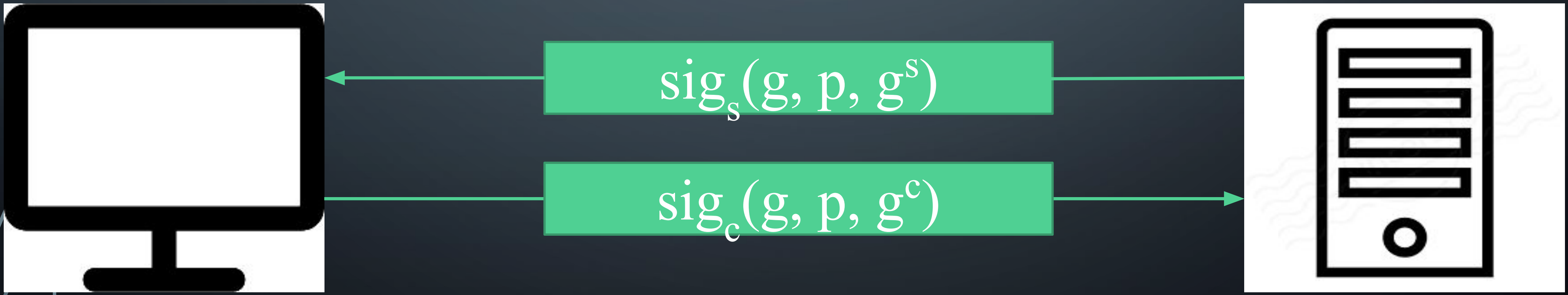


Pre-master: g^{cs} mod p

Continue…

Ephemeral Diffie-Hellman :

- each party sends DH-key signed by its private key
- receiving party verify the signature
- public keys for verification are exchanged using RSA/DSS



$\text{sig}_s(g, p, g^s)$

$\text{sig}_c(g, p, g^c)$

Pre-master: g^{cs}

Continue…

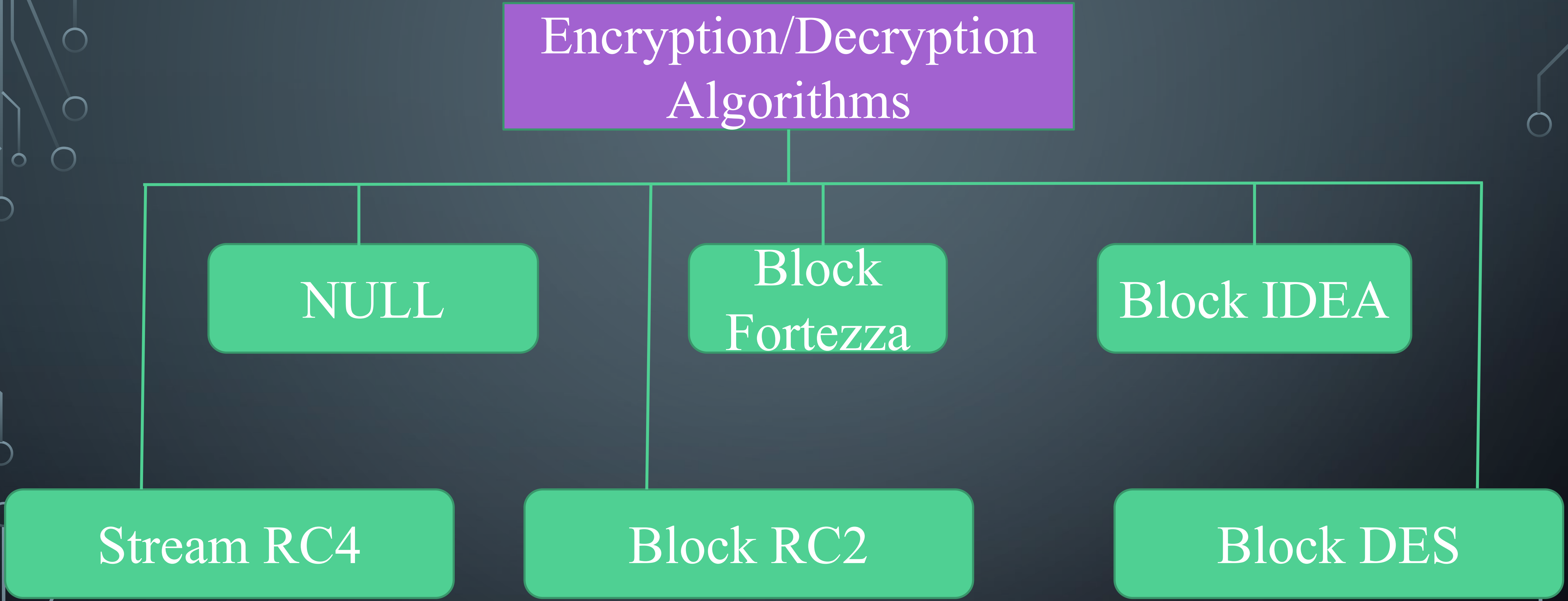
Fixed Diffie-Hellman :

- all entities in a group prepare fixed DH parameters(g,p)
- fixed half-key (g^x)

Fortezza :

- derived from Italian word for fortress
- it is a family of security protocols developed for Defense Department

Continue…



Encryption/Decryption Algorithms

NULL

Block Fortezza

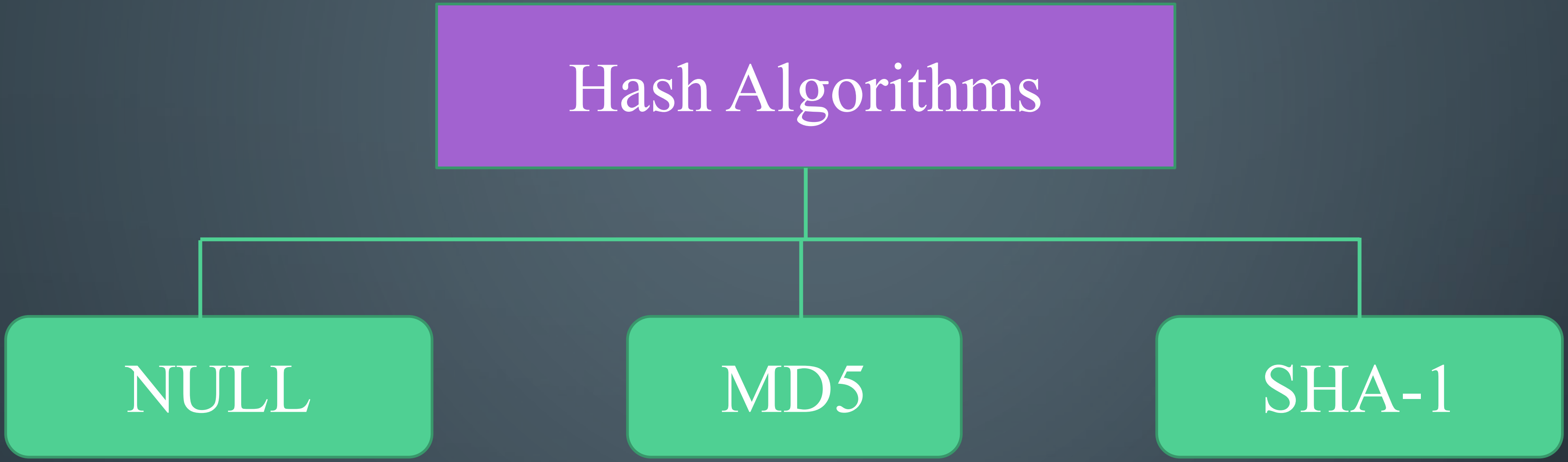
Block IDEA

Stream RC4

Block RC2

Block DES

Continue…



- **Cipher Suite :**

Combination of key exchange, hash and encryption algorithms defines cipher suite for each SSL session

Continue…

❖**Sessions and Connections:**

✔Session is an association between a client and server

✔After session establishment, two parties have common information like session id, certificate authentication, compression method, master secret

✔To exchange data, establishment of session is necessary but not sufficient

✔Need to create connection between two party

Continue…

- ✔Session can consist of many connections
- ✔Session can be suspended and resumed again
- ✔Session is defined by session state, a set of parameters established between server and client
- ✔Connection is defined by connection state, a set of parameters established between two peers

REFERENCE BOOK:

CRYPTOGRAPHY AND NETWORK SECURITY – BEHROUZ A FOROUZAN, DEBDEEP MUKHOPADHYAY